REQUEST FOR COMMENT RESPONSE

Guidelines 07/2020 on the concepts of controller and processor in the GDPR

European Data Protection Board

19 October 2020

I. INTRODUCTION

In response to the European Data Protection Board's (EDPB) request for comment on new guidelines for the concepts of controller and processor within the General Data Protection Regulation (GDPR), CrowdStrike offers the following views.

We approach this topic from the standpoint of a leading cloud-native cybersecurity provider that defends international operating enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is based on CrowdStrike's role as a processor in terms of Article 4(8) of the GDPR in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

We commend the EDPB for seeking to provide additional clarity on the data controller/processor paradigm, and for enabling stakeholders, including within industry, to provide views. As a practical matter, we periodically encounter confusion on these topics among global customers and prospects applying these concepts to sometimes abstract technical functions. Further, in addition to GDPR, technological advancements over the past few years have raised new questions about what types of activities constitute which designation. Now is an appropriate time to clarify such matters.

This comment does not seek to address every issue raised in the new Guidelines. We only raise a few points most pertinent to emerging cloud computing and cybersecurity issues. We focus in particular on the Guidelines' sections 44-57, 69, and 79-82.

Definition of Controller.

We recommend that the EDPB provide further criteria for defining when an entity is acting as a controller. Specifically, we believe the definition of Controller provided thus far by the EDPB lacks clarity on the following four points:

- The legal relationship between the the controller and the data subject, whose personal data is processed;
- The duty to ensure that it has a legal basis for the processing towards the data subject;
- The question whether the commissioned processing must be for the sole benefit of the controller; and
- The direct accountability for compliance with the GDPR regarding the processing of personal data towards the data subject.

The European Commission is fostering Artificial Intelligence, including Machine Learning, but it is not clear as to whether use of such technologies is viewed as a processor or controller activity. Today, both controllers and processors deploy AI in a variety of applications, consistent with their roles. Accordingly, we recommend that the EDPB provide clarification on this topic.

Section 44-57. In general, we believe that these articles of the EDPB's guidance clarify issues relevant to joint controllers.

> **Section 69.** *Joint controllership may also be excluded in a situation where several entities use a shared database or a common infrastructure, if each entity independently determines its own purposes.*
>
> *Example: Marketing operations in a group of companies using a shared database:*
>
> *A group of companies uses the same database for the management of clients and prospects. Such database is hosted on the servers of the mother company who is therefore a processor of the companies with respect to the storage of the data. Each entity of the group enters the data of its own clients and prospects and processes such data for its own purposes only. Also, each entity decides independently on the access, the retention periods, the correction or deletion of their clients and prospects' data. They cannot access or use each other's data. The mere fact that these companies use a shared group database does not as such entail joint controllership. Under these circumstances, each company is thus a separate controller.*

In general, we share the EDPB's opinion on how common infrastructure affects the degree to which a joint controller arrangement may or may not exist. The reality is that globalized markets often necessitate managing customer accounts on a global scale. Invariably, this may require access to the same customer data by local and headquarter-based employees, for example, whereby a group of companies is not using a shared database solely for unique purposes, as independent entities, but instead for cross-collaboration amongst global peers. Accordingly, joint controllership may in fact exist even where several entities use a shared database or common infrastructure.

> **Section 79.** *Acting "on behalf of" also means that the processor may not carry out processing for its own purpose(s). As provided in Article 28(10), a processor infringes the GDPR by going beyond the controller's instructions and starting to determine its own purposes and means of processing.*

> *The processor will be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.*

The EDPB's guidance could further improve by better reflecting the realities of big data analytics in which data may be processed on behalf of the controller but for the benefit of a wider community. Today, many data controllers leverage efficient cloud-native technologies to achieve efficiencies and better environmental practices by processing data once and creating derivative advantages for many. This is especially true in cybersecurity, where patterns detected from a cyber attack against one controller can be used to protect many controllers against data breaches. Accordingly, the EDPB should clarify that processing "on behalf of" a data controller may also provide benefits "on behalf of" other controllers where a data controller agrees.

> **Section 81.** *The EDPB notes that a service provider may still be acting as a processor even if the processing of personal data is not the main or primary object of the service, provided that the customer of the service still determines the purposes and means of the processing in practice. When considering whether or not to entrust the processing of personal data to a particular service provider, controllers should carefully assess whether the service provider in question allows them to exercise a sufficient degree of control, taking into account the nature, scope, context and purposes of processing as well as the potential risks for data subjects.*

A wide variety of commercial IT services create the potential for incidental data processing activities. Services adapt and change over time--including scope, features, functionality, and so on--as users' needs change and providers innovate and iterate on their offerings. These changes sometimes affect processing activities. Throughout these evolutions, the overall purpose of processing activities is generally the most consistent variable.

As the European Commission has articulated, Artificial Intelligence will fuel economic growth and innovation in the years to come.[1] Already today, at CrowdStrike, we use AI to detect and prevent ever-evolving cyber attack techniques in real-time. CrowdStrike's Falcon Platform enables data controllers to leverage the machine events generated by their enterprise endpoints to better fulfill data protection obligations related to adopting appropriate security safeguards. It is through the use of AI that the Falcon Platform is designed to detect previously-unknown ransomware and other not-before-seen infiltration techniques. Protecting data, including personal data, from breaches is the primary objective of the Falcon Platform, rather than the processing of personal data. Accordingly, this technological reality means that a processor remains a processor regardless of the use of innovative technologies.

In general, the use of AI entails applying an algorithm against data in real time, in CrowdStrike's case, largely metadata and other forms of derivative data. Data science models are updated frequently at both the endpoint and cloud-level in order to defeat constantly evolving environmental changes and modifications in threat actor tactics, techniques, and procedures. CrowdStrike's responsiveness to these changing factors is essential; it enables us to prevent data breaches and other compromises that may pose significant adverse privacy implications.

[1] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Data controllers understand the purpose of CrowdStrike's evolving processing activities--to prevent breaches--even throughout updates and changes to our services and solutions. But they do not exercise a high degree of control over adjustments and modifications to CrowdStrike's data science models, which are frequent, or related incidental processing activities.

> **Article 82.** *As stated above, nothing prevents the processor from offering a preliminary defined service but the controller must make the final decision to actively approve the way the processing is carried out and/or to be able to request changes if necessary.*

With incidental data processing activities in particular, it may not be possible to change processing elements without eroding or destroying the solution's efficacy, which again potentially weakens defenses against possible threat actor activity that could result in severe data breaches. Further, to the extent that processing modes or methods apply broadly across service providers' and processors' customer bases, it may not be possible to request changes on an individual customer basis. In these instances, controllers should be enabled to make the determination that an overriding data protection interest should offset any notion of reviewing and approving minor adjustments in real-time, which is common, and would quickly become impractical. In other words, where the same interest is being met and the purpose and means of the processing are consistent with this interest, then data controllers should be able to provide deference with regard to technical details.

III. CONCLUSION

In general, we think these Guidelines helpfully clarify data protection responsibilities and obligations. In several cases, clarifying controller definitions and issues related to AI, as outlined above, can help ensure that the EDPB's efforts promote rather than hinder innovation and ultimately lead to stronger protections for controllers and subjects.

The example cases beginning with Article 22 and used throughout the document offer helpful insight into industry verticals and functions. The application of AI in various services has now become commonplace, well beyond the cybersecurity use cases described above. We believe using AI data processing as a test case for certain articles will make the Guidelines clearer and more robust. We therefore encourage the EDPB to consider including such cases going in future guidance documents.

Thank you again for soliciting feedback on these critical issues from stakeholders, and please contact us if you wish to explore these topics in greater detail.

IV. ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events

per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Privacy and public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Dr. Christoph Bauswein CIPP/E
Director & Counsel, Data Protection & Policy

Email: policy@crowdstrike.com

###